Attorney's Docket No.: 5577-223 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Bruton, et al. Confirmation No.: 2267
Serial No.: 09/773,811 Group Art Unit: 2152
Filed: January 31, 2001 Examiner: Truong, Lan Dai T
For: **METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SELECTIVELY ALLOWING USERS OF A MULTI-USER SYSTEM ACCESS TO NETWORK RESOURCES**

Date: April 25, 2007

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION
I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on April 25, 2007.

Michele P. McMahan

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

Sir:

This *Appeal Brief* is filed pursuant to the *Notice of Appeal to the Board of Patent Appeals and Interferences* filed concurrently herewith in response to the *Final Office Action* ("Final Action") mailed March 20, 2007.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. § 1.136(a). Any additional fees believed to be due may be charged to Deposit Account No. 09-0461.

Real Party In Interest

The real party in interest is assignee International Business Machines Corporation, Armonk, New York.

Related Appeals and Interferences

Appellants are aware of no appeals or interferences that would be affected by the present

appeal.

Status of Claims

Claims 1-9 and 14-28 stand finally rejected. Claims 10-13 have been cancelled. Appellants appeal the rejections of Claims 1-9 and 14-28. The attached Appendix A presents the claims at issue on this appeal.

Status of Amendments

Appellants filed an Amendment on March 6, 2006 in response to the first Office Action of December 8, 2005. The March 6, 2006 Amendment was entered. After a Final Office Action was issued on May 26, 2006, Appellants filed a Request for Reconsideration on June 20, 2006. This Request for Reconsideration, which did not include any claim amendments, was not entered. Appellants filed a Notice of Appeal along with a Pre-Appeal Request for Review on July 19, 2006. In response, a third (non-final) Office Action was issued on October 31, 2006, which withdrew all of the previous rejections, but added new rejections as well. Appellants filed a Request for Reconsideration on December 19, 2006, which was entered. The Final Office Action from which the present appeal is taken was then issued on March 20, 2007.

The attached Appendix A presents the claims on appeal (Claims 1-9 and 14-28) as amended in Appellants' Amendment of March 6, 2006 (which was the only paper submitted by Appellants that amended the pending claims).

Summary of Claimed Subject Matter

Independent Claim 1 is directed to a method for selectively allowing access to resources in a network such as, for example, IP network **10** in Figure 1 of the present application. Each of the resources (e.g., workstations **40-49**, mainframe computers **20-22**, etc. in Figure 1) in the network **10** is assigned to one of a plurality of security zones (e.g., **Zones A-D** in Figure 2) based on a level of security sensitivity of the resource. (Specification at page 12, lines 8-15; *see also* Specification at page 12, lines 22-31). Pursuant to the method of Claim 1, a request from a user of a multi-user system is received. (Specification at page 19, lines 18-30; Figure 6, block **400**;

see also Specification at page 11, lines 16-29). This request is a request to transmit a message over the network to one of the resources. (Specification at page 19, lines 18-21). In response to the request, the security zone that is associated with the resource that is to receive the message is identified. (Specification at page 19, lines 18-21; Figure 6, block **402**; *see also* Specification at page 17, lines 3-13). A determination is made as to whether the user is authorized access to the identified security zone. (Specification at page 19, line 33 through page 20, line 5; Figure 6, block **404** *see also* Specification at page 17, lines 13-16). If so, the message is forwarded over the network. (Specification at page 20, lines 5-10; Figure 6, blocks **406** and **408** *see also* Specification at page 17, lines 16-19).

Claim 14 is directed to a system for selectively allowing access to resources in a network such as, for example, IP network **10** in Figure 1 of the present application. Each of the resources (e.g., workstations **40-49**, mainframe computers **20-22**, etc. in Figure 1) in the network **10** is assigned to one of a plurality of security zones (e.g., **Zones A-D** in Figure 2) based on a level of security sensitivity of the resource. (Specification at page 12, lines 8-15; *see also* Specification at page 12, lines 22-31). The system of Claim 14 includes means for receiving a request originated from a user of a multi-user system (e.g., mainframe computers **20-22** in Figure 1) to transmit a message over the network to one of the resources. (Specification at page 19, lines 18-30; Figure 6, block **400**; *see also* Specification at page 11, lines 16-29). The means for receiving this request may comprise a communications process such as, for example, TCP/IP kernel **140** of Figure 3 of the present application. (Specification at page 14, lines 11-27). The system further includes means for identifying the security zone that is associated with the resource to which the message is to be sent. (Specification at page 19, lines 18-21; Figure 6, block **402**; *see also* Specification at page 17, lines 3-13). This means for identifying the security zone may comprise, for example, a data structure such as security data structure **190** of Figure 3 of the present application or the network resource-to-security zone mapping table **200** of Figure 4 of the present application. (Specification at page 14, line 28 through page 15, line 33). The system further includes means for determining if the user is authorized access to the identified security zone. (Specification at page 19, line 33 through page 20, line 5; Figure 6, block **404** *see also*

Specification at page 17, lines 13-16). This means for determining if the user is authorized access may comprise, for example, a data structure such as data structure **132** in the RACF **130** (see Figure 3) which is accessed by a process such as, for example, TCP/IP kernel **140** of Figure 3. (Specification at page 17, lines 3-16). The system further includes means for forwarding the message over the network if it is determined that the user is authorized access to the identified security zone. (Specification at page 20, lines 5-10; Figure 6, blocks **406** and **408** *see also* Specification at page 17, lines 16-19). The means for forwarding the message may comprise, for example, a communications process such as TCP/IP kernel **140**. (Specification at page 17, lines 17-20).

Claim 19 is directed to a computer program product for selectively allowing access to resources in a network such as, for example, IP network **10** in Figure 1 of the present application. Each of the resources (e.g., workstations **40-49**, mainframe computers **20-22**, etc. in Figure 1) in the network **10** is assigned to one of a plurality of security zones (e.g., **Zones A-D** in Figure 2) based on a level of security sensitivity of the resource. (Specification at page 12, lines 8-15; *see also* Specification at page 12, lines 22-31). The computer program product of Claim 19 includes a computer-readable storage medium having computer-readable program code embodied therein. (Specification at page 5, line 23 through page 7, line 12). The computer-readable program code includes computer program product means for receiving a request originated from a user of a multi-user system (e.g., mainframe computers **20-22** in Figure 1) to transmit a message over the network to one of the resources. (Specification at page 19, lines 18-30; Figure 6, block **400**; *see also* Specification at page 11, lines 16-29). The computer program product means for receiving this request may comprise a communications process such as, for example, TCP/IP kernel **140** of Figure 3 of the present application. (Specification at page 14, lines 11-27). The computer-readable program code further includes computer program product means for identifying the security zone that is associated with the resource to which the message is to be sent. (Specification at page 19, lines 18-21; Figure 6, block **402**; *see also* Specification at page 17, lines 3-13). This computer program product means for identifying the security zone may comprise, for example, a data structure such as security data structure **190** of Figure 3 of the

present application or the network resource-to-security zone mapping table **200** of Figure 4 of the present application. (Specification at page 14, line 28 through page 15, line 33). The computer-readable program code further includes computer program product means for determining if the user is authorized access to the identified security zone. (Specification at page 19, line 33 through page 20, line 5; Figure 6, block **404** *see also* Specification at page 17, lines 13-16). This computer program product means for determining if the user is authorized access may comprise, for example, a data structure such as data structure **132** in the RACF **130** (see Figure 3) which is accessed by a process such as, for example, TCP/IP kernel **140** of Figure 3. (Specification at page 17, lines 3-16). The computer-readable program code further includes computer program product means for forwarding the message over the network if it is determined that the user is authorized access to the identified security zone. (Specification at page 20, lines 5-10; Figure 6, blocks **406** and **408** *see also* Specification at page 17, lines 16-19). The computer program product means for forwarding the message may comprise, for example, a communications process such as TCP/IP kernel **140**. (Specification at page 17, lines 17-20).

Independent Claim 24 is directed to a method for selectively allowing a user of a multi-user system access to resources in a network such as, for example, IP network **10** in Figure 1 of the present application. Pursuant to the method of Claim 24, a message is received over the network **10** from one of the resources. (Specification at page 22, lines 23-32). The message is addressed to a process running on the multi-user system that is associated with the user. (Specification at page 22, lines 23-32). A security zone that is associated with the resource is identified. (Specification at page 22, line 32 through page 23, line 3). A determination is made as to whether or not the user is authorized access to the identified security zone. (Specification at page 23, lines 3-9). If so, the message is forwarded to the process. (Specification at page 23, lines 9-11).

Independent Claim 25 is directed to a data processing system for selectively allowing access to a plurality of resources in a network. The data processing system of Claim 25 includes a data processing device such as, for example, mainframe computer **20** of Figure 1 that is connected to a first network (e.g., network **10** of Figure 1) that includes a plurality of networked

resources. (Specification at page 9, line 22 through page 10, line 34). The data processing system further includes a plurality of workstations (e.g., workstations **40-42** in Figure 1) that are configured to execute applications on the data processing device **20**. (Specification at page 9, line 22 through page 10, line 34). The data processing system also includes a first data structure (e.g., mapping table **200** of Figure 4) that specifies at least one security zone from a plurality of security zones that is associated with each of the plurality of networked resources. (Specification at page 15, line 4 through page 17, line 2). Finally, the data processing system includes a second data structure (e.g., data structure **132** of Figures 3 and 5) that specifies the respective security zones to which a different users of the data processing device may have access. (Specification at page 17, line 28 through page 18, line 2).

Grounds of Rejection to be Reviewed on Appeal

The rejections of Claims 1-9 and 14-28 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,548,649 to Jacobson ("Jacobson") in view of U.S. Patent No. 6,366,912 to Wallent et al. ("Wallent").

Argument

I. Introduction

Claims 1-9 and 14-28 stand rejected as obvious under 35 U.S.C. § 103(a). A determination under Section 103 that an invention would have been obvious to someone of ordinary skill in the art is a conclusion of law based on fact. *Panduit Corp. v. Dennison Mfg. Co.* 810 F.2d 1593, 1 U.S.P.Q.2d 1593 (Fed. Cir. 1987), *cert. denied*, 107 S.Ct. 2187. After the involved facts are determined, the decision maker must then make the legal determination of whether the claimed invention as a whole would have been obvious to a person having ordinary skill in the art at the time the invention was unknown, and just before it was made. *Id.* at 1596. The United States Patent and Trademark Office (USPTO) has the initial burden under § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988).

To establish a *prima facie* case of obviousness, the prior art reference or references when

combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. § 2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. § 2143.01. As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be clear and particular, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

Furthermore, as stated by the Federal Circuit with regard to the selection and combination of references:

> This factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to "[use] that which the inventor taught against its teacher." W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983). Thus the Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency's conclusion....

In re Sang Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002).

Appellants respectfully submit that the pending claims are patentable over Jacobson and Wallen because Jacobson and Wallent, alone or in combination, fail to disclose or suggest all of the recitations of the pending claims and because the reasoning behind such combination has not been established with clear and particular evidence as required by the Federal Circuit. The patentability of the pending claims is discussed in detail hereinafter.

II. The Rejections of Claims 1, 7, 9, 15-17, 19-22 and 28

As noted above, independent Claims 1, 14 and 19 are directed to, respectively, a method, a system and a computer program product for selectively allowing access to a plurality of

resources in a network. The Final Office Action ("Final Action") states that each of Claims 1, 14 and 19 is obvious over Jacobson in view of U.S. Patent No. 6,366,912 to Wallent. (Final Action at 2). The Final Action only provides a response to the arguments raised in Appellants' Request for Reconsideration of December 19, 2006, and otherwise incorporates the rejections from the previous Office Action of October 31, 2006 ("Office Action") rather than repeating the rejections again. Accordingly, throughout this Appeal Brief, reference will be made to both the Final Action and the Office Action as is necessary to explain to rationale for the pending rejections and Appellants contentions regarding why the rationales are not supportable.

With respect to Claims 1, 14 and 19, the Office Action states that Jacobson discloses all of the recitations of Claims 1, 14 and 19 except for the "level of security sensitivity of the resource, and that this missing teaching is provided by Wallent. (Office Action at 4). Appellants respectfully submit that the rejections of Claims 1, 14 and 19 should be reversed for at least the three (3) independent reasons discussed in the following subsections. The arguments below are presented with respect to Claim 1, but it will be understood that due to the correspondence between Claims 1, 14 and 19, each of these arguments apply equally against the rejections of Claims 14 and 19, and that these arguments likewise apply to dependent Claims 7, 9, 15-17, 20-22 and 28.

Claim 1, which is representative of Claims 1, 14 and 19, recites:

> 1. A method for selectively allowing access to a plurality of resources in a network, the method comprising:
>
> receiving a request originated from a user of a multi-user system to transmit a message via the multi-user system over the network to one of the plurality of resources, wherein each of the plurality of resources has been assigned to one of a plurality of security zones based on a level of security sensitivity of the resource;
>
> identifying a one of the plurality of security zones that is associated with the one of the plurality of resources;
>
> determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones; and

forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones.

The Office Action states that (1) the host devices 102-1 through 102-10 of Jacobson comprise the "resources" of Claim 1, (2) the security bridges 104-1 through 104-3 of Jacobson each correspond to the "multi-user system" of Claim 1, (3) that secure zones 108-1 through 108-3 comprise the "plurality of security zones" recited in Claim 1, and (4) that Figure 1 of Jacobson shows each of the "resources" (host devices) being assigned to one of the security zones. (Office Action at 3). As shown in the following sections, however, Jacobson fails to disclose several of the recitations of Claim 1, and Wallent is neither cited as disclosing, nor discloses, the recitations of Claim 1 that are missing from Jacobson. Accordingly, Appellants respectfully submit that the Office Action fails to make a *prima facie* rejection of Claims 1, 14 and 19 under 35 U.S.C. § 103(a), and hence, the rejections of independent Claims 1, 14 and 19, as well as the rejections of Claims 7, 9, 15-17, 20-22 and 28 which depend therefrom, should be reversed.

A. Jacobson Does Not Disclose Identifying a Security Zone that is Associated with a Resource to Which a Message is to be Sent

The second clause of Claim 1 recites "identifying a one of the plurality of security zones that is associated with the one of the plurality of resources." The Office Action states that Jacobson discloses grouping the host devices 102-1 through 102-10 into the plurality of secure zones 108-1 through 108-3. (Office Action at 3). While Appellants agree that Jacobson does group the host devices 102-1 through 102-10 into zones 108-1 through 108-3, this is not what is recited in Claim 1. Instead, what the combination of the first two clauses of the body of Claim 1 recite is "identifying a . . . security zone that is associated with the resource" where **the resource is the resource that is to receive the message from the user**. Jacobson does not attempt to identify a particular one of the security zones 108-1 through 108-3 that is associated with a resource in response to receiving a request to transmit a message to that resource. Thus, the rejection of Claim 1 should be reversed for this reason.

The Final Action argues that Jacobson at Col. 6, lines 53-65, discloses a "method for using filter tables which included [sic] in the security zone bridge to identifying [sic] wherefrom (security zone hosts) the data packet sent from and whereto (secure zone hosts) the received data packets are processed to." (Final Action at 2, ¶ 5). However, there is simply no teaching or suggestion that the "filter tables" of Jacobson are used to identify a particular security zone that is associated with a resource that is to receive a message from a user as is recited in the first two clauses in the body of Claim 1. In fact, the various filter tables of Jacobson are filtering based on (1) Ethernet protocol (*see* Jacobson at Col. 6, lines 8-12), (2) IP protocol (*see* Jacobson at Col. 6, lines 46-48) or (3) IP addresses of hosts and/or bridges (*see* Jacobson at Col. 6, lines 62-65). As is clear from a careful review of Jacobson, none of these filter tables have anything to do with **identifying a security zone that is associated with a resource**. Instead, the filter tables filter based on a protocol or an IP address. Accordingly, the rejection of Claims 1, 7, 9, 14-17, 19-22 and 28 should be reversed.

B. Jacobson Does Not Determine if a User is Authorized Access to an Identified Security Zone

The third clause of the body of Claim 1 recites "determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones" (herein the "determining recitation" of Claim 1). The Office Action states that the "identification filter table" at each security bridge 104-1 through 104-3 of Jacobson is "used to identify if the request [sic] transmitted packet is authorized to access one of [the] security host device[s]." Appellants note that Jacobson does not describe any "identification filter table" as stated in the Office Action, but instead discusses several "filter tables" and several other "identification tables." While the Office Action does not clearly indicate which of these tables forms the basis for the pending rejection of Claims 1, 7, 9, 14-17, 19-22 and 28, Appellants submit that the discussion below demonstrates that none of these tables disclose the "determining recitation" of Claims 1, 7, 9, 14-17, 19-22 and 28.

In particular, as noted above, the "filter tables" described in Jacobson are the Ethernet protocol filter table 214, the IP protocol filter table 220, and the IP address filter table 222.

(Jacobson at Col. 6, lines 4-65). Jacobson does not disclose or suggest that these "filter tables" are used to "determine[e] if **the user** of the multi-user system is **authorized access to the identified one of the plurality of security zones**" as recited in the third clause of the body of Claim 1. Instead, the filter tables of Jacobson appear to be used to determine if a "normal data packet has been received" and if not, the packet is deleted. (*See, e.g.,* Jacobson at Col. 6, lines 13-28). There is simply no disclosure or suggestion in Jacobson that the "filter tables" filter based on whether or not a **user is authorized access to a particular security zone**. To the contrary, filter tables 214 and 220 appear to **filter based on the protocol types of particular packets**, while filter table 222 appears to filter out packets with IP addresses associated with particular hosts and/or bridges, but does so **without reference to any particular security zone**. (*See, e.g.,* Jacobson at Col. 6, lines 7-19, 41-48 and 62-65). **In fact, the exemplary "filter tables" disclosed in Figures 6-8 of Jacobson clearly show that the filtering is performed solely on either protocol types or IP addresses as opposed to based on whether or not a user is authorized access to a particular security zone**. Thus, the discussion of the "filter tables" of Jacobson fails to disclose or suggest the "determining" recitation of Claim 1.

Similarly, the two "identification tables" discussed in Jacobson – namely the remote secure zone host identification table 230 and the local secure zone host identification table 236 – are not used to "determine[e] if the user of the multi-user system is authorized access to the identified one of the plurality of security zones" as recited in the third clause of the body of Claim 1. Instead, the identification tables 230 and 236 are used in determining the source and/or destination zone of a particular packet in order to determine, for example, whether encryption and/or decryption operations should be performed on the packet. The description at Columns 7 and 8 of Jacobson thus clearly shows that neither identification table 230 nor identification table 236 are used to determine if a user is authorized access to a security zone, let alone to determine if a user is authorized access to an **identified** security zone that is associated with the resource to which the user is sending a message as recited in Claim 1. Accordingly, the rejections of Claims 1, 7, 9, 14-17, 19-22 and 28 should also be reversed for this reason.

The Final Action argues that (1) the "user" of independent Claims 1, 14 and 19 can be either a person or a device and (2) that Jacobson discloses "using security bridges to determine if the data packets are sent from 'a secure zone hosts' [sic] which share functionality with 'the authorized user'; if it is, the security bridge then 'processes' which share functionality with 'forwarding' as claimed the received data packets [sic] to its desired destination secure zone hosts." (Final Action at p. 3, ¶ 6, citing to Col. 4, lines 10-67 of Jacobson). However, nowhere does Jacobson teach or disclose that the security bridges 104-1 through 104-3 are used to determine if a user is authorized access to a security zone associated with a resource to which the user is seeking to send a message. In fact, the security bridges of Jacobson appear to primarily be involved with determining whether or not messages need to be encrypted or decrypted. (*See, e.g.,* Jaconson at Col. 3, lines 31-43). In any event, Appellants respectfully submit that neither the Office Action nor the Final Action identifies any passage from Jacobson which discloses or suggests that the bridges 104-1 through 104-3 of Jacobson determine if a user is authorized access to a security zone associated with a resource to which the user is seeking to send a message as recited in Claims 1, 7, 9, 14-17, 19-22 and 28, and hence the rejections of these claims should also be reversed for this additional reason.

C. Jacobson Does Not Disclose Forwarding a Message Only if it is Determined that the User is Authorized Access to the Identified Security Zone

The last clause in the body of Claim 1 recites "forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones." The Office Action states that Col. 7, lines 1-67, Col. 8, lines 1-48 and Col. 15, lines 1-15 of Jacobson discloses this recitation of Claim 1. (Office Action at 4). In particular, the Office Action states that the security bridges 104-1 through 104-3 of Jacobson forward "authorized install/or view request" packets – which are deemed to be the equivalent of the "message" of Claim 1 – to the desired security zone host device 102-1 through 102-10. (Office Action at 4). Appellants respectfully submit that the cited

portions of Jacobson also fail to disclose the last clause of Claim 1 for at least two separate reasons.

As an initial matter, what the last clause of Claim 1 recites is that the message is forwarded "only if it is determined that the **user is authorized access to the identified . . . security zone**." In contrast, the cited portion of Jacobson states that the local bridge "determines if the user is authorized to install or view the item in the local bridge in a manner similar to that described earlier for determining from the distribution authorization request packet if the user is authorized to distribute an item to a remote bridge." (Jacobson at Col. 15, lines 21-25). The earlier referenced portion of Jacobson, in turn, recites:

> [T]he bridge manager determines whether the user is authorized to perform the bridge local install or view operation. This is done by comparing the user's i.d. and password for accessing local bridge 104-1 with those stored in authorization table 244 and looking up the user's authorization level in the authorization table 244.

(Jacobson at Col. 10, lines 22-28). Thus, in Jacobson, whether or not a user is allowed to install or view items contained in the bridge library 216 is based on whether the user – as identified by an i.d. and a password – has a sufficient **authorization level** as opposed to being based on a determination as to whether or not the user is authorized access to a security zone that has been identified **as being associated with the resource to which the message is being sent** as recited in Claim 1.

More importantly, the network management operations described in Column 15 of Jacobson for installing and/or viewing items in the bridge library are operations that are performed by the "user" of Jacobson. (*See* Jacobson at Col. 15, line 6). As noted above, Jacobson states that these operations are performed in a manner similar to bridge management operations described earlier in Jacobson. (Jacobson at Col. 15, lines 22-26). The earlier description of the bridge management operations makes clear that the "user" referred to in Jacobson is "user 246" which is depicted in Fig. 2.[1] As shown in Fig. 2, the **user terminal 246 is**

[1] Fig. 2 of Jacobson includes a typographical error in that the "user terminal" is labeled 248 and the "serial interface" is labeled 246, whereas in the text of Jacobson the user is referred to as "user 246" and the serial interface is referred to as "serial interface 248."

part of the network security bridge 104-1. Accordingly, the operations for viewing and/or installing items in library 216 have nothing to do with **receiving a request from a user of a multi-user system to transmit a message over a network** as recited in Claim 1, but instead involve a user performing management operations on security bridge 104-1 by logging onto a user terminal present at the security bridge. Accordingly, Jacobson fails to disclose or suggest the last clause of Claim 1 for this independent reason.

The Final Action appears to take the position that Col. 4, lines 10-67 of Jacobson discloses both the "determining" and "forwarding" recitations of Claim 1. (*See* Final Action at p. 3, ¶ 6). This appears to be a new grounds of rejection, as the position taken in the Office Action, which is incorporated by reference into the Final Action, was that the discussion at Col. 7, lines 1-67, Col. 8, lines 1-48 and Col. 15, lines 1-15 in Jacobson of the "authorized install/or view request" packets discloses the "forwarding" recitation of Claim 1. (*See* Office Action at 4). In any event, Col. 4, lines 10-67 of Jacobson clearly do not disclose or suggest "forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones." Thus, the rejection of Claims 1, 7, 9, 14-17, 19-22 and 28 should be reversed for this reason as well.

Thus, for each of the above reasons, Appellants respectfully submit that the rejections of Claims 1, 7, 9, 14-17, 19-22 and 28 should be reversed.

II. The Rejection of Claims 24 and 28

The Office Action states that Claim 24 is rejected for the same reasons that Claim 1 was rejected. (Office Action at 4). After Appellants pointed out that Claims 1 and 24 contain significantly different recitations, the Examiner, **for the first time**, provided the alleged basis for rejecting Claim 24 in the **Final** Action. (*See* Final Action at p. 5, ¶ 10). Appellants have reviewed the alleged grounds for the rejection of Claim 24 and also respectfully submit that those grounds do not provide a proper basis for the rejection.

In particular, the Final Action states that Jacobson discloses a method for receiving a message over a network that is addressed to a process running on a multi-user system that is

associated with a user. (Final Action at p. 5, ¶ 10). While the Final Action states that the "network security bridges" of Jacobson correspond to the "multi-user system of Claim 24, the Final Action does not even attempt to identify what elements of Jacobson correspond to the recited "process running on the multi-user system" or the associated "user." Appellants respectfully submit that Jacobson does not teach that messages are received at the network security bridges that are addressed to a process running on the network security bridge that is associated with a user of the network security bridge. Accordingly, the rejection of Claim 24 should be withdrawn for this reason

The Final Action further states that the "filter tables" of Jacobson are used to identify the security zone associated with the resource to which the received message is addressed. (Final Action at p. 5, ¶ 10). However, as discussed above with respect to the rejection of Claims 1, 7, 9, 14-17, 19-22 and 28, there is absolutely no teaching or suggestion in Jacobson that the filter tables disclosed therein are used in this manner, and Appellants respectfully submit that the cited portions of Jacobson certainly do not provide any such disclosure.

Additionally, neither the Office Action nor the Final Action explain where the last two clauses of the body of Claim 24 can be found in the cited art. Accordingly, the rejection of Claim 24 should also be reversed for each of these reasons, as should the rejection of Claim 28 which depends therefrom.

III. The Rejection of Claim 25

Claim 25 recites:

> 25. A data processing system for selectively allowing access to a plurality of resources in a network, comprising:
>
> a data processing device, the data processing device connected to a first network that includes a plurality of networked resources;
>
> a plurality of workstations that are configured to execute applications on the data processing device;
>
> a first data structure that specifies at least one security zone from a plurality of security zones that is associated with each of the plurality of networked resources, wherein each of the plurality of security zones represents a distinct level of security

sensitivity; and

a second data structure that specifies the respective security zones to which a plurality users of the data processing device may have access.

The Office Action states that the "host devices" of Jacobson are equivalent to the "data processing device" of Claim 25; that the "remote security zone Host ID table" comprises the "first data structure" of Claim 25; that the "authorization table" of Figure 12 of Jacobson comprises the "second data structure" recited in Claim 25, and that "communications between the host devices" comprise the plurality of workstations recited in Claim 25. (Office Action at 5). Appellants also respectfully submit that the cited portions of Jacobson do not correspond to the recitations of Claim 25.

For example, the rejection of Claim 25 indicates that the host devices comprise the "data processing device" of Claim 25 and that communications between the host devices comprise the "plurality of workstations" of Claim 25. What Claim 25 recites, however, is a "plurality of workstations that are **configured to execute applications on the data processing device**." Appellants respectfully submit that the cited portions of Jacobson do not indicate that the host devices are configured to execute applications on each other and, as such, communications between the host devices does not disclose or suggest the "plurality of workstations" of Claim 25. Therefore, the rejection of Claim 25 should be withdrawn for at least this reason.

Appellants also submit that the Host ID table of Jacobson does not correspond to the "first data structure" of Claim 25. The remote secure zone host ID table, which is depicted in Figure 9 of Jacobson, maps the IP address of host devices 102-3 through 102-7 to their corresponding security bridge 104-2 or 104-3. (Jacobson at Col. 7, lines 25-33). As such, the host ID table maps the host devices to a particular **security bridge** as opposed to mapping networked resources to particular **security zones**, and hence does not correspond to the "first data structure" of Claim 25.

Appellants further submit that the "authorization table" of Figure 12 of Jacobson does not disclose or suggest the "second data structure" of Claim 25. Instead, as discussed above, the "authorization table" 244 of Jacobson specifies the types of operations that particular users may

perform on a selected one of the security bridges 104-1 through 104-3. (*See, e.g.*, Jacobson at Col. 10, lines 22-28). As such, the authorization table clearly does not specify the respective security zones to which a user may have access, as can clearly be seen by viewing the last column in the authorization table of Figure 12. Thus, the failure of Jacobson to disclose the second data structure provides a third, independent basis for withdrawal of the rejection of Claim 25.

The Final Action appears to modify the rejection of Claim 25 by relying on Wallent as disclosing "inter-processing between remote computer and remote web server." (Final Action at p. 4, ¶ 8). Appellants respectfully submit that this argument clearly does not overcome Appellants showing above that the cited art fails to disclose or suggest the system of Claim 25. In fact, it is unclear how the Examiner is combining Jacobson and Wallent to allegedly arrive at the system of Claim 25, and the rejections do not even attempt to explain why one of skill in the art would have been motivated to combine Jacobson and Wallent in the alleged manner.

Thus, for each of the above reasons, Appellants respectfully submit that the rejection of Claim 25 should also be withdrawn.

IV. The Rejections of Claims 2-6, 8, 18, 23 and 26-27

Claims 2-6, 8, 18, 23 and 26-26 each depend from one of Claims 1, 14, 19 or 25, and hence each claim is patentable over the cited art for at least the reasons that the claim from which it depends is patentable. Appellants also respectfully submit that these claims are independently patentable over the cited art for the reasons provided in the following sections.

A. Claim 2

Claim 2 recites that "the multi-user system comprises a mainframe computer, and wherein the request is originated on a workstation of the mainframe computer." The Office Action states that Jacobson teaches that the "hosts" 102-1 through 102-12 may comprise mainframe computers. (Office Action at p. 6). However, as discussed above, in rejecting Claim 1, the Office Action takes the position that it is the **bridges** 104-1 through 104-3, as opposed to the hosts 102-1 through 102-12 that comprise the "multi-user system" of Claims 1 and 2. As such, the rejections of Claims 1 and 2 are internally inconsistent and irreconcilable, providing independent grounds for reversal of the rejection of Claim 2.

B. Claims 3 and 4

Claim 3, which depends from Claims 1 and 2, recites that "the mainframe computer receives the request originated from the user, identifies the one of the plurality of security zones associated with the one of the plurality of resources, and determines if the user is authorized access to the one of the plurality of resources." As noted above, the Office Action states (in rejecting Claim 2) that Jacobson teaches that the "hosts" 102-1 through 102-12 may comprise mainframe computers. (Office Action at p. 6). Thus, in rejecting Claim 3 the Office Action is taking the position that **hosts** 102-1 through 102-1 of Jacobson (1) receive the request originated from the user, (2) identify the one of the plurality of security zones associated with the one of the plurality of resources, and (3) determine if the user is authorized access to the one of the plurality of resources. However, as discussed above, in rejecting Claim 1, the Office Action takes the position that it is the **bridges** 104-1 through 104-3 that perform each of the three steps recited above. As such, the rejections of Claims 1 and 3 are internally inconsistent and irreconcilable, providing independent grounds for reversal of the rejection of Claim 3.

Claim 4 depends from Claim 3, and hence is patentable for at least the reasons that Claim 3 is patentable.

C. Claim 5

Claim 5 recites that "at least one entry in the data structure specifies the security zone associated with a group of the resources in the plurality of resources" and that "identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises identifying the security zone associated with the most specific entry in the data structure that includes the resource." Neither the Office Action nor the Final Action attempts to explain where the recitations of Claim 5 can be found in the cited art, but instead the Office action merely points to the rejection of Claim 1, which does not discuss the recitations of Claim 5. Accordingly, no grounds whatsoever for rejecting Claim 5 have been provided, and thus the rejection of Claim 5 should be reversed for this additional reason.

D. Claim 6

Claim 6 recites that "the identifying and determining steps are performed within the multi-user system." The Office Action points to the rejection of Claim 1 as disclosing the grounds for rejecting Claim 6. However, as noted above, in rejecting Claim 1, the Office Action takes the position that it is the **bridges** 104-1 through 104-3 perform the "identifying" and "determining" steps. However, the rejection of Claim 1 identifies the **hosts** 102-1 through 102-12 as comprising the "multi-user system" of Claim 1. Thus, the rejection of Claim 1 does not support the rejection of Claim 6, but instead merely serves to show that Jacobson clearly does not disclose the method of Claim 6. As such, the rejection of Claim 6 should be reversed on this independent basis.

E. Claim 8

Claim 8 recites that "the identifying and determining steps are performed before any data packets associated with the message are forwarded over the network." The Office Action points to the rejection of Claim 1 as disclosing the grounds for rejecting Claim 8. However, the rejection of Claim 1 in the Office Action does not discuss the recitations of Claim 8, and certainly does not show where those recitations can be found in the cited art. Accordingly, no grounds whatsoever for rejecting Claim 8 have been provided, and thus the rejection of Claim 8 should be reversed for this additional reason.

F. Claims 18 and 23

Claim 18 recites that "at least one entry in the data structure specifies the security zone associated with a group of the resources in the plurality of resources" and that "the means for identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises means for identifying the security zone associated with the most specific entry in the data structure that includes the resource." Claim 23 includes similar recitations. The Office Action does not even attempt to explain where Jacobson discloses the recitations of Claims 18 and 23, but instead just groups these claims together with a number of other claims and then fails to address the actual recitations of Claims 18 and 23. As such, the Office Action

has failed to make even a *prima facie* rejection of Claims 18 and 23, providing an independent basis for reversal of the rejection of these claims.

G. Claim 26

Claim 26 recites that "the first data structure comprises a mapping table that identifies the respective one of the plurality of security zones associated with each of the plurality of networked resources" and that "at least some of the entries in the mapping table are associated with multiple of the plurality of networked resources." The Office Action states that Jacobson at Cols. 5 and 6 discloses the recitations of Claim 26. (Office Action at p. 7). However, the Office Action merely recites the language of Claim 26, and asserts, without support, that various tables from Jacobson correspond to the mapping table of Claim 26. Appellants respectfully submit that Jacobson does not disclose or suggest that the identified tables identify the respective security zones that are associated with each of the networked resources, nor does Jacobson disclose that some of the entries in the tables "are associated with multiple of the plurality of networked resources" as recited in Claim 26. Accordingly, Claim 26 is independently patentable over the cited art for these additional reasons.

H. Dependent Claim 27

Claim 27 recites that the "entries in the mapping table include wildcard characters to specify multiple of the plurality of networked resources with a single entry in the mapping table." The Office Action cites to Figs. 9-12 of Jacobson as disclosing the recitations of Claim 27, but provides no explanation as to how or why these figures teach the recitations. Appellants respectfully submit that a review of Figs. 9-12 makes clear that no wildcard characters are included in the tables, and thus it is equally clear that Jacobson does not disclose the subject matter of Claim 27. Accordingly, the rejection of Claim 27 should be reversed for this additional reason.

V. Conclusion

For each of the above reasons, Appellants respectfully submit that the pending claims are patentable over the cited art, and respectfully request the present application be passed to issuance.

Respectfully submitted,

D. Randal Ayers
Registration No. 40,493

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

CLAIMS APPENDIX

1. A method for selectively allowing access to a plurality of resources in a network, the method comprising:

receiving a request originated from a user of a multi-user system to transmit a message via the multi-user system over the network to one of the plurality of resources, wherein each of the plurality of resources has been assigned to one of a plurality of security zones based on a level of security sensitivity of the resource;

identifying a one of the plurality of security zones that is associated with the one of the plurality of resources;

determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones; and

forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones.

2. The method of Claim 1, wherein the multi-user system comprises a mainframe computer, and wherein the request is originated on a workstation of the mainframe computer.

3. The method of Claim 2, wherein the mainframe computer receives the request originated from the user, identifies the one of the plurality of security zones associated with the one of the plurality of resources, and determines if the user is authorized access to the one of the plurality of resources.

4. The method of Claim 3, wherein the step of identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises accessing a data structure that specifies the security zone associated with each resource in the plurality of resources.

5. The method of Claim 4, wherein at least one entry in the data structure specifies the security zone associated with a group of the resources in the plurality of resources, and

wherein identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises identifying the security zone associated with the most specific entry in the data structure that includes the resource.

6. The method of Claim 1, wherein the identifying and determining steps are performed within the multi-user system.

7. The method of Claim 1, wherein the message forwarded over the network includes a first user identification associated with the multi-user system but does not include a second user identification associated with the user of the multi-user system.

8. The method of Claim 1, wherein the identifying and determining steps are performed before any data packets associated with the message are forwarded over the network.

9. The method of Claim 1, wherein the network is an internet protocol network.

10-13. (Cancelled)

14. A system for selectively allowing access to a plurality of resources in a network, comprising:

means for receiving a request originated from a user of a multi-user system to transmit a message via the multi-user system over the network to one of the plurality of resources, wherein each of the plurality of resources has been assigned to one of a plurality of security zones based on a level of security sensitivity of the resource;

means for identifying a one of the plurality of security zones that is associated with the one of the plurality of resources;

means for determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones; and

means for forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones.

15. The system of Claim 14, further comprising means for associating a security zone with each of the plurality of resources.

16. The system of Claim 15, further comprising means for specifying in advance of receiving the request the security zones to which users of the multi-user system are authorized access.

17. The system of Claim 14, wherein the means for identifying the one of the plurality of security zones associated with the one of the plurality of resources comprise means for accessing a data structure that specifies the security zone associated with each resource in the plurality of resources.

18. The system of Claim 17, wherein at least one entry in the data structure specifies the security zone associated with a group of the resources in the plurality of resources, and wherein the means for identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises means for identifying the security zone associated with the most specific entry in the data structure that includes the resource.

19. A computer program product for selectively allowing access to a plurality of resources in a network, comprising:

a computer-readable storage medium having computer-readable program code embodied in said medium, said computer-readable program code comprising:

computer program product means for receiving a request originated from a user of a multi-user system to transmit a message via the multi-user system over the network to one of the plurality of resources, wherein each of the plurality of resources has been assigned to one of a plurality of security zones based on a level of security sensitivity of the resource;

computer program product means for identifying a one of the plurality of security zones that is associated with the one of the plurality of resources;

computer program product means for determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones; and

computer program product means for forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones.

20. The computer program product of Claim 19, further comprising computer program product means for associating a security zone with each of the plurality of resources.

21. The computer program product of Claim 20, further comprising computer program product means for specifying in advance of receiving the request the security zones to which users of the multi-user system are authorized access.

22. The computer program product of Claim 19, wherein the computer program product means for identifying the one of the plurality of security zones associated with the one of the plurality of resources comprise computer program product means for accessing a data structure that specifies the security zone associated with each resource in the plurality of resources.

23. The computer program product of Claim 22, wherein at least one entry in the data structure specifies the security zone associated with a group of the resources in the plurality of resources, and wherein the computer program product means for identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises computer program product means for identifying the security zone associated with the most specific entry in the data structure that includes the resource.

24. A method for selectively allowing a user of a multi-user system access to a plurality of resources in a network, the method comprising:

receiving a message over the network from one of the plurality of resources that is addressed to a process running on the multi-user system that is associated with the user;

identifying, from a plurality of security zones, a security zone associated with the one of the plurality of resources;

determining if the user is authorized access to the identified security zone; and

forwarding the message to the process only if it is determined that the user is authorized access to the identified security zone.

25. A data processing system for selectively allowing access to a plurality of resources in a network, comprising:

a data processing device, the data processing device connected to a first network that includes a plurality of networked resources;

a plurality of workstations that are configured to execute applications on the data processing device;

a first data structure that specifies at least one security zone from a plurality of security zones that is associated with each of the plurality of networked resources, wherein each of the plurality of security zones represents a distinct level of security sensitivity; and

a second data structure that specifies the respective security zones to which a plurality users of the data processing device may have access.

26. The data processing system of Claim 25, wherein the first data structure comprises a mapping table that identifies the respective one of the plurality of security zones associated with each of the plurality of networked resources, wherein at least some of the entries in the mapping table are associated with multiple of the plurality of networked resources.

27. The data processing system of Claim 26, wherein entries in the mapping table include wildcard characters to specify multiple of the plurality of networked resources with a single entry in the mapping table.

28. The method of Claim 24, wherein the multi-user system identifies the security zone associated with the one of the plurality of resources and determines if the user is authorized access to the identified security zone.

EVIDENCE APPENDIX

No evidence is being submitted with this *Appeal Brief*.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.